HOUSE BILL REPORT
HB 1654

As Reported by House Committee On:
Innovation, Technology & Economic Development

Title: An act relating to the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology.

Brief Description: Concerning the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology.

Sponsors: Representatives Ryu, Shea, Morris, Valdez, Kloba, Fitzgibbon, Appleton, Frame and Tarleton.

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 2/6/19, 2/22/19 [DPS].

Brief Summary of Substitute Bill

- Requires all government entities to follow state law regulating the collection and use of biometric data by state agencies until certain conditions are met.
- Prohibits government use of facial recognition systems to monitor public spaces without probable cause, or to analyze footage obtained from a police body worn camera.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Morris, Slatter, Tarleton, Van Werven and Wylie.

Staff: Yelena Baker (786-7301).

Background:

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Facial Recognition Technology.

Facial recognition is one of several biometric technologies which identify individuals by measuring and analyzing their physiological or behavioral characteristics. Facial recognition generally works by capturing an image, using an algorithm to create a faceprint, or a facial template, and then comparing the captured image to a database of images or a single image in a database. The more similar the environments in which the images are compared, the better a facial recognition system will perform.

Facial recognition technologies can perform a number of functions, including detecting a face in an image, estimating personal characteristics, verifying identity, and identifying an individual by matching an image of an unknown person to a database of known people. Facial recognition systems can generate two types of errors: false positives (generating an incorrect match) or false negatives (not generating a match where one exists).

Facial recognition is used in a variety of consumer and business applications, including safety and security, secure access, marketing, and customer service. In the public sphere, it is more commonly used for law enforcement and security purposes. Additionally, many states, including Washington, use facial recognition technology to identify cases of driver's license fraud by comparing driver's license photos with other images on file.

State Biometric Data Laws.

State law regulating the collection and use of biometric data by state agencies defines "biometric identifier" as any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Several specific types of information are excluded from this definition, including information derived from photographs or physical descriptions, donated organ parts or blood, and information captured in a health care setting.

Unless authorized by law, agencies are prohibited from obtaining a biometric identifier without first providing notice that clearly specifies the purpose and use of the identifier, and obtaining consent specific to the terms of the notice. Agencies that obtain biometric identifiers must establish and follow certain security and privacy policies, including a biometric policy designed to minimize the collection of biometric identifiers. The use and storage of biometric identifiers obtained by agencies must comply with all other applicable state and federal laws and regulations.

Agencies are prohibited from selling biometric identifiers and may only use a biometric identifier consistent with the terms of the notice and consent. Sharing biometric identifiers is permitted only to execute the purposes of the collection consistent with the notice and consent, if sharing is specified in the original consent, or as authorized by law. Biometric identifiers may not be disclosed under the Public Records Act.

Government Surveillance.

The Fourth Amendment of the United States Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and

seizures." Article 1, section 7 of the Washington State Constitution provides, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." These provisions have been interpreted by courts to prohibit the government or a state actor from conducting certain searches of individuals without a warrant issued by a court of competent jurisdiction. This prohibition is enforced by excluding evidence obtained in violation of the warrant requirement, unless an exception applies. However, many kinds of government surveillance are not considered a search requiring a warrant under the federal or state Constitution. This may include surveillance of activities occurring in open fields or in plain view, and sometimes, the government's acquisition of information from a third party. Congress and state legislatures may choose to establish stronger regulations on government surveillance than the floor established by either the federal or state Constitution.

Washington State Academy of Sciences.

Created by the Legislature in 2005, the Washington State Academy of Sciences (Academy) is a nonprofit organization whose principal mission is to investigate, examine, and report on any subject of science referred to the Academy by the Governor or the Legislature. The Governor must provide funding to the Academy for the actual expense of such investigation, examination, and report.

Summary of Substitute Bill:

"Facial recognition" is defined to mean both the automated or semi-automated process by which a person is identified based on the characteristics of their face, and the automated or semi-automated process by which these characteristics are analyzed to determine the individual's sentiment, state of mind, or behavioral propensities, such as the level of dangerousness.

All government entities are required to follow state law regulating the collection and use of biometric data by state agencies until:

- The Attorney General provides a report to the Legislature on whether independent third-party testing shows any statistically significant variation in the accuracy of facial recognition systems on the basis of race, skin tone, ethnicity, gender, or age.
- The Washington Academy of Sciences convenes a diverse task force and delivers a report to the Legislature documenting the potential consequences and the best procurement practices of government use of facial recognition systems.
- The Legislature passes legislation that includes appropriate restrictions on government use of facial recognition.

State and local government agencies are prohibited from using facial recognition systems to monitor public spaces without probable cause, or to use facial recognition to analyze footage obtained from a police body-worn camera.

Facial recognition data gathered in violation of these provisions is considered unlawfully obtained and is inadmissible as evidence in any trial or proceeding before any authority

subject to the jurisdiction of the state of Washington. Unlawfully obtained facial recognition data must be deleted upon discovery.

A person injured by the violations of these provisions may institute proceedings for injunctive relief, declaratory relief, a writ of mandate, or an action to recover actual damages.

Substitute Bill Compared to Original Bill:

The substitute bill:

- modifies the moratorium on government use of facial recognition into the requirement that all government entities follow the procurement practices set forth in state law regulating the collection and use of biometric data by state agencies;
- modifies provisions related to the task force to require that the report documents the potential consequences of government use of facial recognition systems on the civil rights and liberties of all Washingtonians;
- specifies additional types of representatives to be included in the membership of the task force;
- removes the requirement that government entities obtain a warrant in order to use a facial recognition system to monitor public spaces and instead requires probable cause for such use; and
- makes technical revisions to eliminate duplicate language and corrects the reference to the government of China.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) Facial recognition is a game-changing technology that gives the government unprecedented power to automatically identify, locate, and track people based on the images of their faces. This technology poses unique civil rights and civil liberties concerns. Existing law places no limits on the use of facial recognition technology, which is being widely adopted by many agencies in Washington, and which is being used without public knowledge. This bill would allow government use of facial recognition technology only when it can be proven to be unbiased and would create an inclusive task force to have the much-needed discussion about what constitutes acceptable and off-limits uses of this technology.

Facial recognition systems use proprietary programs that are not available for public inspection. Multiple expert studies have shown that facial recognition systems amplify existing biases and are inaccurate at identifying women, people of color, transgender, and gender nonconforming people. Existing field tests of these systems use racially-biased data

sets. In one test, a facial recognition system falsely identified 28 members of Congress, most of whom were people of color, as criminals. Facial recognition technology has been disproportionately used to single out Muslims and other people of color for surveillance without a warrant or a suspicion of criminal activity. The lack of resources for law enforcement is understandable, but using flawed technology that produces false positives would drain law enforcement resources even further.

Even an unbiased face surveillance system alters people's willingness to go about their lives in public or to exercise their constitutional rights because people will want to avoid the possibility of their speech and identity being subjected to scrutiny in public places.

(Opposed) Law enforcement agencies struggle to provide safety to Washingtonians at the most affordable cost, and use they facial recognition technology as a public safety tool. A match by a facial recognition system is used as an investigatory lead, similar to an anonymous tip. Data gathered by facial recognition technology is essential to identifying criminals who commit crimes across different jurisdictions. Discrimination and bias are serious issues in the underlying algorithms.

(Other) In 2012 the Legislature authorized the Department of Licensing (DOL) to use facial recognition technology to prevent identity fraud, and placed a number on safeguards on how the data may be used and shared. Any potential matches are reviewed by staff who have received special training; anyone flagged after staff review is given an opportunity to prove that no identity fraud is occurring. The federal Department of Homeland Security requires the use of facial recognition technology in issuing driver's licenses in order to comply with the security standards set forth in the REAL ID Act. If the DOL is not exempt from the provisions of this bill, it would be unable to issue enhanced driver's licenses.

Facial recognition technology has a number of positive uses, such as reuniting missing children with their families and making passport control more efficient. Regulation of facial recognition systems should be calibrated so as to continue positive uses of the technology and to limit the potential for harmful uses. This bill does not achieve that objective because it blocks many positive uses of facial recognition technology.

Persons Testifying: (In support) Representative Ryu, prime sponsor; Jevan Hutson, Os Keyes, and Katherine Pratt, University of Washington; Shankar Narayan, American Civil Liberties Union of Washington; and Masih Fouladi, Council on American-Islamic Relations.

(Opposed) James McMahan, Washington Association of Sheriffs and Police Chiefs; and Brad Tower, Community Bankers of Washington.

(Other) Beau Perschbacher, Department of Licensing; and Natasha Crampton, Microsoft.

Persons Signed In To Testify But Not Testifying: None.